U.S. Department of Justice

United States Attorney
Southern District of New York

The Silvio J. Mollo Building
One Saint Andrew's Plaza
New York, New York 10007

July 31, 2021

VIA ECF

The Honorable Gregory H. Woods
United States District Judge
Southern District of New York
500 Pearl Street
New York, New York 10007

Re: *United States v. Medghyne Calonge*, 20 Cr. 523 (GHW)

Dear Judge Woods:

The Government respectfully submits this letter brief in response to the defendant Medghyne Calonge's revised proposed jury instructions (the "Revised Proposal") and accompanying letter (the "Letter" or "Ltr.") dated July 28, 2021 (Dkt. No. 44). The defendant's proposals consist principally of requests that the Court instruct the jury that, in order to convict, the jury must find that the defendant damaged a specific computer and circumvented technological restrictions. The requests are incorrect as a matter of law, and the defendant points to no court that has ever instructed a jury as such in a case involving the charges at issue here. The requests should be denied.[1]

The defendant first asserts "that under 18 U.S.C. § 1030(a)(5)(A) and (B), the damage must be to the specific 'protected computer' to which the program was allegedly transmitted (for 5(A)) or accessed without authorization (for 5(B))." Ltr. at 1. This apparently novel interpretation finds no support in the statutory language, authoritative sources, or the caselaw. Sections 1030(a)(5)(A) and (B) both speak in terms of "a" protected computer and nowhere include a requirement that the protected computer receiving the program, information, code, or command (in the case of Section 1030(a)(5)(A)) or the protected computer accessed without authorization (in the case of Section 1030(a)(5)(B)) be the same exact computer that is damaged. Likewise, neither Sand nor the Ninth Circuit model instruction includes any such requirement. *See* Sand, *Modern Federal Jury Instructions, Instr.* 40A-31 and 40A-39, and Ninth Circuit model instructions 8.100 and 8.101.

At first glance, the defendant appears to find some support in *United States v. Grupe*, 2018 WL 775358, at *2 (D. Minn. Feb. 8, 2018), which states that the district court in that case instructed

[1] The defendant's Revised Proposal consists of a Word document in which the defendant added, in track changes, proposed changes to Request Nos. 3-6, 8-11, and 14. The Government, in a separate filing also made today on ECF, has included in comments its position on the defendant's changes to those same requests.

a jury that satisfaction of the third element of a Section 1030(a)(5)(A) offense required proof that "the transmission caused damage to *the* protected computer." *See* Revised Proposal Req. No. 3 n. 2 (emphasis added). But review of the *actual* jury instructions in that case reveals that the jury was in fact instructed that the transmission must cause damage to "a" protected computer. *See United States v. Grupe*, 17 Cr. 90 (PJS/DTS), at 6 (Dkt. No. 61), attached hereto as Exhibit A. In other words, the appearance of "the" rather than "a" in the opinion appears to be a mistake. The other case cited by the defendant, *United States v. Goodyear*, likewise lends no support to the defendant's request. 795 F. App'x 555, 559 (10th Cir. 2019) (requiring proof that "(1) Defendant knowingly caused the transmission of *a* program, information, code, or command to *a* protected computer; and (2) Defendant, as a result of such conduct, intentionally caused damage to *a* protected computer without authorization.") (emphasis added).

Additionally, the defendant's novel interpretation of the statute—which has absolutely no basis in the text of the statute—would effectively neuter Section 1030(a)(5), the primary violation in Section 1030 aimed at criminal activity causing damage to computer systems. In the world of the Internet and networked computing (which existed well before the passage of the Computer Fraud and Abuse Act in 1986), where data is regularly stored in the cloud and beyond the immediate computer systems being accessed, the defendant's interpretation of the statute would render the violation meaningless, as it would insulate individuals who attempt to intentionally damage data stored in the cloud through the acts prohibited by Section 1030(a)(5)(A).

Second, the defendant urges the Court to adopt a requirement that proof of circumvention of technological access restrictions is required. *See* Ltr. 2-3; Revised Proposal Req. Nos. 6, 9. Again, the language of the statutes requires nothing of the sort, and the model instructions do not either. *See* Sand, *Modern Federal Jury Instructions, Instr.* 40A-31 and 40A-39, and Ninth Circuit model instructions 8.100 and 8.101. In terms of Section 1030(a)(5)(A), such a requirement makes no sense when the question of whether the defendant's access to a victim's computer system was authorized is entirely irrelevant. *See United States v. Thomas*, 877 F.3d 591, 598 (5th Cir. 2017) ("We conclude that Section 1030(a)(5)(A) prohibits intentionally damaging a computer system when there was no permission to engage in that particular act of damage."); *United States v. Yücel*, 97 F. Supp. 3d 413, 422 (S.D.N.Y. 2015) ("A defendant thus causes damage without authorization when he has not been permitted by the victim to cause that damage."); *United States v. Stratman*, No. 4:13-CR-3075, 2013 WL 5676874, at *1 (D. Neb. Oct. 18, 2013) ("[O]ne who is authorized to access a system, but not authorized to damage it, violates the statute by intentionally damaging it 'without authorization.'"); *see also B & B Microscopes v. Armogida*, 532 F. Supp. 2d 744, 758 (W.D. Pa. 2007) ("Section 1030(a)(5)(A)(i) is not predicated upon unauthorized access of a protected computer. Instead, it is predicated upon unauthorized damage to a computer."); *In re America Online, Inc.*, 168 F. Supp. 1359, 1371 (S.D. Fla. 2001) (distinguishing sections 1030(a)(5)(B)-(C) from section 1030(a)(5)(A) and stating that "Congress did not intend § 1030(a)(5)(A) to apply only to outsiders who lack authorization."). The plain text of section 1030(a)(5)(A) does not require unauthorized access in any form, it just requires that the defendant intentionally cause damage to a computer system.

While Section 1030(a)(5)(B), unlike Section 1030(a)(5)(A), does require that the defendant access a protected computer without authorization, the Government has found no case (and the defendant offers none) in which a court has required circumvention of technological restrictions

to satisfy that element. Tellingly, the defendant relies entirely on cases involving other provisions of the Computer Fraud and Abuse Act, which focused primarily on an issue not raised here concerning what it means to "exceed authorized access," (a statutory term that is completely absent from Section 1030(a)(5)) and advocacy in an amicus brief the Supreme Court recently considered and specifically declined to address or adopt. *See Van Buren v. United States*, 141 S. Ct. 1648, 1659 n.8 (2021); *see also United States v. Valle*, 807 F.3d 508 (2d Cir. 2015) (concerning 18 U.S.C. § 1030(a)(2)); *United States v. Nosal*, 676 F.3d 854, 865 (9th Cir. 2012) (en banc) (concerning 18 U.S.C. § 1030(a)(4)); *Van Buren v. United States*, 141 S. Ct. 1648 (concerning 18 U.S.C. § 1030(a)(2)). The Second Circuit has found that there is no need to instruct a jury on the meaning of authorization. *See also United States v. Morris*, 928 F.2d 504, 511 (2d Cir. 1991) ("Since the word [authorization] is of common usage, without any technical or ambiguous meaning, the Court was not obliged to instruct the jury on its meaning."). And there is no reason to stray from that direction here, where the Government's theory of the defendant's Section 1030(a)(5)(B) violation is so straightforward and accessible to the jury. The Government contends that, by virtue of her termination from the victim company, the defendant no longer had *any* authority (*i.e.*, she was "without authorization") to access the victim company's system, regardless of whether, through oversight, her access was not formally revoked and she therefore still had login credentials that enabled her to access and damage that system.

In sum, the Court should decline the defendant's invitation to make new law and instead reject the defendant's recent proposals.

Respectfully submitted,

AUDREY STRAUSS
United States Attorney

By: _____
Timothy V. Capozzi
Louis A. Pellegrino
Assistant United States Attorneys
(212) 637-2404 / 2617

cc: Martin Cohen, Esq., Federal Defenders of New York (by ECF)